Allowable Subject Matter

1. Claims 1-9, 11-24, 26-42 and 44-56 are allowed.

2. Claims 10, 25 and 43 are cancelled.

3. Applicant's amendment including amended claims filed on 06/01/2010 has been entered.

EXAMINER'S AMENDMENT

4. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Jasper Kwoh on 7/26/2010.

The application has been amended as follows:

AMENDMENTS TO THE CLAIMS

Claim 1. (Currently Amended) A computer-implemented method for managing user access information for access to one or more database network nodes by a user, the method comprising:

storing database user authorization in a central directory that is associated with one or more network nodes, the database user authorization comprising a user role associated with a collection of locally defined roles and associated users, wherein the user role in the central directory assigns user privileges to the user as defined by the locally defined roles contained within the user role, wherein the database user authorization is stored as one or more data objects in the central directory;

storing database user authentication information;

receiving the user role at a local database network node from the central directory; locally defining, by using a processor, a locally defined role for assigning the user privileges specific to a local database network node for a local scope of access at the local database network node, wherein the locally defined role is locally defined by processing at the local database network node the user role that is received from the central directory and the user privileges granted by the locally defined role is given to the user based at least in part upon user's association with the user role as provided by the user role such

that the locally defined role has a different scope of access than another locally defined role defined by processing the same user role at another local database network node;

receiving an access request from the user for the local database network node;

authenticating the user using a shared schema based at least in part upon the database user authentication information, wherein the shared schema comprises a schema that is accessible by a plurality of users and the plurality of users are mapped to the shared schema on the local database network node such that the plurality of users do not need their own accounts on the local database network node;

granting the user privileges on the local database network node based at least in part upon the shared schema and the ~~local policy~~ locally defined role; and

storing the user privileges in a volatile or non-volatile computer-usable medium or displaying the user privileges on a display device.

Claim 19. (Currently Amended) A computer system including a processor for managing user access information for access to one or more database network nodes by an enterprise user, comprising:

a LDAP directory;

one or more local database network nodes for which user access is sought, wherein the one or more local database network nodes are associated with the LDAP directory;

a volatile or non-volatile computer-usable medium for storing user access information data objects in the LDAP directory, the user access information data objects comprising authentication and authorization information, wherein the authorization information comprises an enterprise role associated with a collection of locally defined roles and associated users, wherein the enterprise role in the LDAP directory assigns user privileges to the enterprise user as defined by the locally defined roles contained within the enterprise role; and

the processor for locally defining a locally defined role for assigning the user privileges specific to a local database network node for a local scope of access at the local database network node, wherein the locally defined role is locally defined by processing at the local database network node the enterprise

role that is received from the ~~central~~ LDAP directory and the user privileges granted by the locally defined role ~~is~~ are given to the enterprise user based at least in part upon user's association with the ~~user~~ enterprise role as provided by the ~~user~~ enterprise role such that the locally defined role has a different scope of access than another locally defined role defined by processing the same enterprise role at another local database network node.

Claim 39. (Currently Amended) A computer program product that includes a volatile or non-volatile non-transitory computer-usable medium usable by a processor, the medium having stored thereon a sequence of instructions which, when executed by said processor, causes said processor to execute a process for managing user access information for access to one or more database network nodes by a user, the process comprising:

storing database user authorization in a central directory that is associated with one or more network nodes, the database user authorization comprising a user role

associated with a collection of locally defined roles and associated users, wherein the user role in the central directory assigns user privileges to the user as defined by the locally defined roles contained within the user role, wherein the database user authorization is stored as one or more data objects in the central directory;

storing database user authentication information;

receiving the user role at a local database network node from the central directory;

locally defining a locally defined role for assigning the user privileges specific to a local database network node for a local scope of access at the local database network node, wherein the locally defined role is locally defined by processing at the local database network node the user role that is received from the central directory and the user privileges granted by the locally defined role is given to the user based at least in part upon user's association with the user role as provided by the user role such that the locally defined role has a different scope of access than another locally defined role defined by processing the same user role at another local database network node;

receiving an access request from the user for the local database network node;

authenticating the user using a shared schema based at least in part upon the database user authentication information, wherein the shared schema comprises a schema that is accessible by a plurality of users and the plurality of users are mapped to the shared schema on the local database network node such that the plurality of users do not need their own accounts on the local database network node;

granting the user privileges on the local database network node based at least in part upon the shared schema and the ~~local policy~~ locally defined role; and

storing the user privileges or displaying the user privileges on a display device.

AMENDMENTS TO THE SPECIFICATION

In the specification, the paragraphs beginning on page 66, line 3 are replaced with the following paragraphs:

The term "computer-usable medium," as used herein, refers to any medium that provides information or is usable by the processor(s) 1907. Such a medium may take many forms, including~~, but not limited to,~~ non-volatile~~,~~ and volatile ~~and transmission~~ media. Non-volatile media, i.e., media that can retain information in the absence of power, includes the ROM 1909. Volatile media, i.e., media that can not retain information in the absence of power, includes the main memory 1908. ~~Transmission media includes coaxial cables, copper wire and fiber optics, including the wires that comprise the bus 1906. Transmission media can also take the form of carrier waves; i.e., electromagnetic waves that can be modulated, as in frequency, amplitude or phase, to transmit information signals. Additionally, transmission media can take the form of acoustic or light waves, such as those generated during radio wave and infrared data communications.~~

Common forms of computer-usable media include, for example: a floppy disk, flexible disk, hard disk, magnetic tape, any other magnetic medium, CD-ROM, any other optical medium, punchcards, papertape, any other physical medium with patterns of holes, RAM, ROM, PROM (i.e., programmable read only memory), EPROM (i.e., erasable programmable read only memory), including FLASH-EPROM, any other memory chip or cartridge, ~~carrier waves,~~ or any other non-transitory medium from which a

processor 1907 can retrieve information. Various forms of computer-usable media may be involved in providing one or more sequences of one or more instructions to the processor(s) 1907 for execution. The instructions received by the main memory 1908 may optionally be stored on the storage device 1910, either before or after their execution by the processor(s) 1907.

In the specification, the paragraph beginning on page 67, line 1 is replaced with the following paragraph.

Each processing unit may also include a communication interface 1914 coupled to the bus 1906. The communication interface 1914 provides two-way communication between the respective user stations 1924 and the host computer 1922. The communication interface 1914 of a respective processing unit transmits and receives electrical, electromagnetic or optical signals that include data streams representing various types of information, including instructions, messages and data. A communication link 1915 links a respective user station 1924 and a host computer 1922. The communication link 1915 may be a LAN 1826, in which case the communication interface 1914 may be a LAN card. Alternatively, the communication link 1915 may be a PSTN 1828, in which case the communication interface 1914 may be an integrated services digital network (ISDN) card or a modem. Also, as a further alternative, the communication link 1915 may be a wireless network 1830. A processing unit may transmit and receive messages, data, and instructions, including program, i.e., application, code, through its respective communication link 1915 and communication interface 1914. Received program code may be executed by the respective processor(s) 1907 as it is received, and/or stored in the storage device 1910, or other associated non-volatile media, for later execution. In this manner, a processing unit may receive messages, data and/or program code ~~in the form of a carrier wave~~.

5. The following is an examiner's statement of reasons for allowance:

The present invention relates to computer systems, and more particularly, to a method and mechanism for managing access information in a distributed computing environment, such as a distributed database environment.

The claimed invention (claim 1 as representative) recites features such as:"…the database user authorization comprising a user role associated with a collection of locally defined roles and associated users, wherein the user role in the central directory assigns user privileges to the user as defined by the locally defined roles contained
within the user role."

The prior art of record (Cohen et al. US 6178511 B1) teach a single sign-on (SSO) mechanism to enable a given user to access a target application on a target resource in a distributed computer enterprise. One or more configuration directives each identifying a given logon process and any associated methods required to access the target application on the target resource are stored in a preferably global-accessible database (CIM), (abstract, Cohen et al.).

Moriconi et al. (US 6158010) teach a system and method for maintaining security in a distributed computing environment comprises a policy manager located on a server for managing and distributing a security policy, and an application guard located on a client for managing access to securable components as specified by the security policy (abstract, Moriconi et al.).

Bains et al. (US 5579222) teach an improved system for administration of license terms for a software product on the network, having an arrangement, for tracking software product usage, with one of the computers acting as a license server (abstract, Bains et al.).

Ferguson et al. (US 20020082818 A1) teach a data model that allows for modeling of all information relating to a computer network to be conveniently stored in a database in a manner which minimizes the effort associated with the addition of new devices to the network and maximizes software code reuse (abstract, Ferguson et al.).

Gavrila et al. (US 20020026592 A1) teach a method for automatic permission management in centralized and distributed operating systems using role-based access control that supports selective and multiple instantiations of roles, multiple inheritance of permission and membership, and provides scalable and efficient distribution, review, and revocation of permissions and access authorization (abstract, Gavrila et al.).

Franklin et al. (US 20010023440 A1) teach that a directory services system includes a resource object, such as an application object for accessing a resource associated with the resource object (abstract, Franklin et al.).

McNabb et al. (US 6289462 B1) teach a system and method for providing a trusted server which controls access to the execution of processes by applying file level extended sensitivity label attributes. The attributes are utilized to restrict execution of processes that are requested by comparing the extended attributes in addition to using standard file permission authorization. The system additionally may be used to provide controlled execution of commercially available software (abstract, McNabb et al.).

The prior arts however do not teach the database user authorization comprising a user role associated with a collection of locally defined roles and associated users, wherein the user role in the central directory assigns user privileges to the user as defined by the locally defined roles contained within the user role.

Hence, the prior arts of record do not anticipate nor render obvious the claimed invention. Thus, claim 1 is allowable over the prior arts of record. Claims 2-9, 11-18 and 52-56 are allowed because of the combination of additional limitations and the limitations listed above.

- As per claim 19, the prior arts of record also do not teach that the authorization information comprises an enterprise role associated with a collection of locally defined roles and associated users, wherein the enterprise role in the LDAP directory assigns user privileges to the enterprise user as defined by the locally defined roles contained within the enterprise role as recited in claim 19.

Thus claim 19 is allowable over the prior arts of record. Claims 20-24 and 26-38 are allowed because of the combination of additional limitations and the limitations listed above.

- Claim 39 recites same patentable features as in claim 1. Thus claim 39 is allowable over the prior arts of record. Claims 40-42 and 44-51 are allowed because of the combination of additional limitations and the limitations listed above.
- Thus, claims 1-9, 11-24, 26-42 and 44-56 are allowable over the prior arts of record.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DIPAKKUMAR GANDHI whose telephone number is (571)272-3822. The examiner can normally be reached on 9:00 AM - 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, JEFFREY GAFFIN can be reached on (571)272-4146. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/DIPAKKUMAR GANDHI/
Examiner, Art Unit 2117

/Jeffrey A Gaffin/
Supervisory Patent Examiner, Art Unit 2100